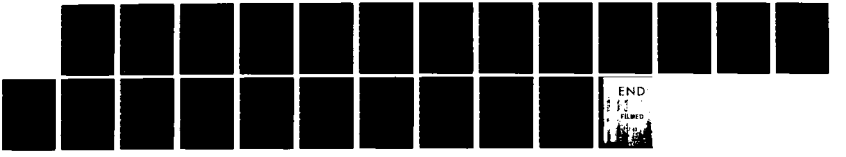
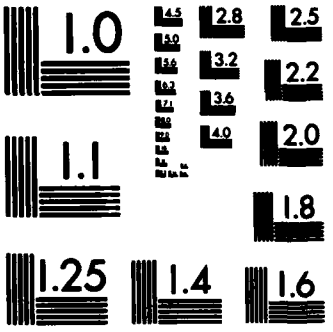
AD-A133 851 FAST CONVOLUTION ALGORITHMS AND ASSOCIATED VHSIC ARCHITECTURES(U) UNIVERSITY OF SOUTHERN CALIFORNIA LOS ANGELES DEPT OF ELECTRI... I S REED 23 MAY 83 1/1

UNCLASSIFIED AFOSR-TR-83-0748 AFOSR-80-0151 F/G 9/5 NL





MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS-1963-A

(2)

REPORT DOCUMENTATION PAGE

READ INSTRUCTIONS BEFORE COMPLETING FORM

1. REPORT NUMBER: AFOSR-TR- 83-0748	2. GOVT ACCESSION NO.: AD-A133 851
3. RECIPIENT'S CATALOG NUMBER	
4. TITLE (and Subtitle): FAST CONVOLUTION ALGORITHMS AND ASSOCIATED VHSIC ARCHITECTURES	5. TYPE OF REPORT & PERIOD COVERED: FINAL 4/15/80 - 4/15/83
	6. PERFORMING ORG. REPORT NUMBER
7. AUTHOR(s): Professor Irving S. Reed, Principal Investigator	8. CONTRACT OR GRANT NUMBER(s): AFOSR 80-0151
9. PERFORMING ORGANIZATION NAME AND ADDRESS: University of Southern California, Electrical Engineering Department, University Park, Los Angeles, CA 90089-0272	10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS: PE61102F; 2304/A3
11. CONTROLLING OFFICE NAME AND ADDRESS: Department of the Air Force, Air Force Office of Scientific Research (AFSC) /NM, Bolling AFB, DC 20332	12. REPORT DATE: May 23, 1983
	13. NUMBER OF PAGES: 21
14. MONITORING AGENCY NAME & ADDRESS (if different from Controlling Office)	15. SECURITY CLASS. (of this report): Unclassified
	15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT (of this Report)

Approved for public release; distribution unlimited.

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

18. SUPPLEMENTARY NOTES

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

Finite field, Mersenne prime, Fermat number, primitive element, number-theoretic transform, cyclic convolution, polynomial transform, digital filtering, Reed-Solomon codes, 3-D reconstruction, $|\omega|$-filter, neurosurgery, inner product computer, Galois switching theory, cryptography.

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

In this final report the publications of the past five years that were supported by this grant are listed. There are 48 papers and 6 Ph.D. dissertations listed in the final report. These publications fall into five categories or groups. A brief summary of each group is given. Finally an abstract of each paper/dissertation is given in the report.

AFOSR-TR- 83-0748

FINAL TECHNICAL PROGRESS REPORT

1. GRANT TITLE AND NUMBER:

FAST CONVOLUTION ALGORITHMS AND ASSOCIATED VHSIC ARCHITECTURES, AFOSR 80-0151

2. CONTRACTOR: University of Southern California

3. PERIOD COVERED: 4/15/80 4/15/83

4. REPORT PREPARED BY: Professor Irving S. Reed, Principal Investigator

5. DATE PREPARED: May 23, 1983

6. DOCTORAL THESES WRITTEN WITH SUPPORT OF THIS GRANT:

(1) Yik San Kwoh, Application of Finite Field Transforms to Image Processing and X-Ray Reconstruction, Ph.D. granted January 1977.

(2) K.Y. Liu, Efficient Digital Transform Algorithms and Architectures for Signal Processing and Error Correcting Codes, Ph.D. granted June 1977.

(3) C.M. Chang, 3-D Reconstruction and the Technique of X-Ray Computerized Tomography, Ph.D. granted July 1979.

(4) David W. Kravitz, The Application of Finite Polynomial Rings to Number-Theoretic Crypto-Systems, Ph.D. granted May 1982.

(5) Howard M. Shao, Techniques for Signal Processing of Image Data, Ph.D. granted May 1983.

(6) C.-S. Yeh, Parallel VLSI Architectures of Signal and Communication Processors, Ph.D. granted June 1983.

7. A FIVE YEARS TECHNICAL RESEARCH SUMMARY:

(1) Methods to Find Primitive Elements in Certain Finite Fields

New methods are developed to find elements of order $2^{p+1}p$ and $2^k n$ in the finite field $GF(q^2)$, where $q = 2^p-1$ is a Mersenne prime, p is a prime number, and n is a divisor of $2^{p-1}-1$ [18,20,50]. Also a new method is developed to find primitive elements in the finite field $GF(q^2)$ of q^2 elements [30,36,50].

(2) Fast Transform Algorithms and Applications

Number-theoretic transforms are developed to compute one-dimensional cyclic convolutions [3-5,13-17,21,37]. One advantage of such transforms over the usual discrete Fourier transform is it uses only integer arithmetic. Also a hybrid algorithm is developed to perform convolutions [21, 27, 40]. Moreover, a fast polynomial transform is developed to compute two-dimensional cyclic convolutions [35,39]. These new transform techniques can be applied to digital filtering in speech, radar, communications and image processing [1,44-47,53-54].

(3) Transform Decoder for Correcting Both Errors and Erasures of the Reed-Solomon Error-Correcting Code

A fast number-theoretic transform technique is developed for the encoding and decoding of Reed-Solomon codes [9-10,22-23,28-29,38]. This new transform technique for decoding errors and erasures of a (255,223) Reed-Solomon codes over $GF(2^8)$ is faster than the conventional Reed-Solomon decoding technique [31,33,38]. If such a Reed-Solomon code is concatenated with a Viterbi decoded convolutional code it can be used to reduce the

signal-to-noise ratio required to meet the specified bit-error rate for deep space applications and military applications in the presence of ECM. This transform decoder for Reed-Solomon codes can be used in multiple-user communication systems [8,12,46].

(4) 3-D Reconstruction for X-rays and Radar

New algorithms are developed for x-ray reconstruction [2,7,16, 49,51]. This algorithm improves the computational speed and resolution of x-ray reconstruction. A generalized $|\omega|$-filter is developed to reduce x-ray dosage and to enhance the edge of reconstructured pictures [6,26, 49,51]. A Weiner filter is used to improve the image quality of an object in the 3-D reconstruction by a weighted average of successive overlapping two-D sections of the object [24,32,34,51]. A computer program is written for a specially designed head mounted frame that is used in neurosurgery [4

(5) Inner Product Computers, Galois Switching Theory and Cryptography

The inner product computer is a special-purpose computational unit intended to be used in conjunction with a general-purpose computer to perform numerical processing tasks. The hardware implementation of an inner product computer is designed, analyzed and compared with a general-purpose computer [11]. In [19], the general structure of the Galois switching theory is developed. A cryptographic construct is developed for the use of computer system security [43, 52]. The crypto-structure can be used in modern multi-user secure communications networks.

8. REFERENCES

A. Published Papers and Abstracts

1. I.S. Reed, T.K. Truong, Y.S. Kwoh and E.L. Hall, "Image Processing by Transforms Over a Finite Field," IEEE Trans. on Computers, Vol. C-26, No. 9, September 1976, pp. 874-881.

Abstract - A transform analogous to the discrete Fourier transform is defined on the Galois field GF(p), where p is a prime of the form $k \times 2^n+1$, where k and n are integers. Such transforms offer a substantial variety of possible transform lengths and dynamic ranges. The fast Fourier transform (FFT) algorithm of this trasnform is faster than the conventional radix-2 FFT. A transform of this type is used to filter a two-dimensional picture (e.g., 256×256 samples), and the results are presented with a comparison to the standard FFT. An absence of roundoff errors is an important feature of this technique.

2. I.S. Reed, Y.S. Kwoh, T.K. Truong, and E.L. Hall, "X-Ray Reconstruction by Finite Field Transforms," IEEE Trans. on Nuclear Science, Vol. NS-24, No. 1, February 1977, pp. 843-849.

Abstract - In this paper a fast transform method is used to perform the convolution of the Shepp and Logan filter with the projection data. To perform these convolutions at optimal computational speed and accuracy, a fast Fourier transform (FFT) algorithm is developed over a finite or Galois field GF(q) of integers instead of the usual field of complex numbers. GF(q) is the field of integers modulo q where q is a prime of the form $k \cdot 2^n+1$. Important features of this computational technique to tomography are both a high computational speed and an absence of round-off errors.

3. S.W. Golomb, I.S. Reed and T.K. Truong, "Integer Convolutions Over the Finite Field $GF(3 \cdot 2^n+1)$," SIAM Journal on Applied Mathematics, Vol. 32, No. 2, March 1977, pp. 356-365.

Abstract - An analogue of the discrete Fourier transform is defined in the finite field $GF(q_n)$, where q_n is a prime of the form $3 \times 2^n+1$. The arithmetic operations performing this transform require integer multiplication, addition, subtraction, and bit shifts of a word. It is shown that the fast Fourier transform algorithm can be utilized to yield fast convolution of integer numbers without round-off error.

4. K.Y. Liu, I.S. Reed and T.K. Truong, "Fast Algorithm for Computing Complex Number-Theoretic Transforms," Electronic Letters, Vol. 13, No. 10, 12th May, 1977, pp. 278-280.

Abstract - A high-radix f.f.t. algorithm for computing transforms over $GF(q^2)$, where q is a Mersenne prime, is developed to implement fast circular convolutions. This new algorithm requires substantially fewer multiplications than the conventional f.f.t.

5. K.Y. Liu, I.S. Reed and T.K. Truong, "Fast Algorithm for Complex Integer Transforms," IEEE Trans. on Acoustics, Speech, and Signal Processing, Vol. ASSP-25, No. 5, October 1977, pp. 450-452.

Abstract - In this correspondence both high-radix and real-valued input FFT algorithms are applied to transforms over the finite field $GF(q^2)$, where q is a Mersenne prime. Such transforms can be used to implement fast circular convolutions without roundoff error. Of particular interest is a new radix 8 FFT algorithm, which requires fewer multiplications than the conventional radix 8 FFT algorithm.

6. Y.S. Kwoh, I.S. Reed and T.K. Truong, "A Generalized $|\omega|$-Filter for 3-D Reconstruction," IEEE Trans. on Nuclear Science, Vol. NS-24, No. 5, October 1977, pp. 1990-1998.

Abstract - In this paper a study and generalization is made of the previous $|\omega|$-filters. It extends the important filters of Ramachandran and Lakshiminarayanan, and Shepp and Logan to a class of generalized $|\omega|$-filters. A generalized $|\omega|$-filter can be chosen to have both good accuracy and a flexibility to cope with noise. A detailed comparison is made among the different possible filter shapes with respect to their responses to simulated data and noise. Finally in this paper it is demonstrated that a substantial reduction in the x-ray exposure time can be accomplished by choosing the appropriat generalized $|\omega|$-filter.

7. Y.S. Kwoh, I.S. Reed and T.K. Truong, "Back Projection Speed Improvement for 3-D Reconstruction," IEEE Trans. on Nuclear Science, Vol. NS-24, No. 5, October 1977, pp. 1999-2005.

Abstract - The Fourier convolution algorithm has been used to reconstruct a 3-D density function. The method involves a particular choice of weighting function to convolve with projection data sets scanned through various angles from 0 to π. The convolved data are then back projected to obtain a 2-D image. A 3-D reconstruction is obtained as a stack of 2-D images. Because the new tomographic machines have much finer resolution, the number of projection data to be processed is considerably more than with the early models. The amount of data to be processed makes critical the need for improvements in both the speed as well as the accuracy.

A first step toward speed improvement is to use a finite field transform to perform the convolutions. This was shown previously by the authors to be, in fact, a worthwhile effort.

Another and most time-consuming part of the reconstruction algorithm is the so-called back-projection algorithm. The purpose of this paper is to present a method for speeding-up the back-projection algorithm by cutting down the computational time by a factor of two.

8. H. Murakami, I.S. Reed and L.R. Welch, "Transform Decoder of Reed-Solomon Codes for Multiple-User Communication Systems Using a Direct Sum of Galois Fields," IEEE Trans. Inform. Theory, Vol. IT-23, No. 6, November 1977, pp. 675-683.

Abstract - Encoding and decoding algorithms for Reed-Solomon codes based on Fourier-like transforms on finite field and finite rings are discussed. Classes of codes are proposed for two different types of multiple-user communication systems: a multichannel communication systems and a multiaccess communication system. For the first system, a fast decoding algorithm is developed that uses transforms on a finite ring which is isomorphic to a direct sum of Galois fields. For the second system, an efficient (in terms of information rate) coding scheme is proposed which utilizes a direct sum of Galois fields.

9. K.Y. Liu, I.S. Reed and T.K. Truong, "High-Radix Transforms for R-S Codes Over Fermat Primes," IEEE Trans. Inform. Theory, Vol. IT-23, No. 6, November 1977, pp. 776-778.

Abstract - It is shown that a high-radix fast Fourier transform (FFT) with generator $\gamma = 3$ over $GF(F_n)$, where $F_n = 2^{2^n}+1$ is a Fermat prime, can be used for encoding and decoding of Reed-Solomon (RS) codes of length 2^{2^n}. Such an RS decoder is considerably faster than a decoder using the usual radix 2 FFT. This technique applies most ideally to a 16-error-correcting, 256-symbol RS code of 8 bits being considered currently for space communication applications. This special code can be encoded and decoded rapidly using a high-radix FFT algorithm over $GF(F_3)$.

10. I.S. Reed, R.A. Scholtz, T.K. Truong and L.R. Welch, "The Fast Decoding of Reed-Solomon Codes Using Fermat Theoretic Transforms and Continued Fractions," IEEE Trans. on Inform. Theory, Vol. IT-24, No. 1, January 1978, pp. 100-106.

Abstract - It is shown that Reed-Solomon (RS) codes can be decoded by using a fast Fourier transform (FFT) algorithm over finite fields $GF(F_n)$, where F_n is a Fermat prime, and continued fractions. This new transform decoding method is simpler than the standard method for RS codes. The computing time of this new decoding algorithm in software can be faster than the standard decoding method for RS codes.

11. E.S. Swartzlander, B.K. Gilbert and I.S. Reed, "Inner Product Computers," IEEE Trans. on Computers, Vol. C-27, No. 1, January 1978, pp. 21-31.

Abstract - The inner product computer is a special-purpose computational unit intended to be used as an adjunct to a general-purpose digital computer to perform numerical processing tasks which previously exceeded the capacity of the general-purpose computer. The algorithmi structure of the inner product is briefly reviewed in the first section of this paper. Methods are described for computing the inner product of complex vectors with a series of four real inner products. Several hardware implementations of the inner product computer are described and then compared in terms of speed and complexity; a figure of merit is developed to simplify the comparison. The utility of this computational unit is demonstrated via the examination of a large-scale reconstruction (computerized tomography) arising in the biomedical sciences. Finally, a comparison is given of the size of a general-purpose computer required to execute a large-scale processing task with that of an inner product computer to execute the same task. The inner product computer greatly reduces computational costs for the solution of a large class of problems, including computerized tomography, image restoration, weather forecasting, and economic modeling.

12. H. Murakami and I.S. Reed, "Multi-Channel Convolutional Coding Systems Over a Direct Sum of Galois Fields," IEEE Trans. on Inform. Theory, Vol. IT-24, No. 2, March 1978, pp. 205-212.

Abstract - Classes of codes for a multichannel communication system are considered. A fast algorithm is developed to calculate syndromes of multichannel linear systematic codes, including both block and convolutional codes, by using a direct sum of Galois fields.

13. I.S. Reed and T.K. Truong, "A Fast DFT Algorithm Using Complex Integer Transforms," Electronic Letters, Vol. 14, No. 6, March 16th 1978, pp. 191-193.

Abstract - For certain large transform lengths, Winograd's algorithm for computing the discrete Fourier transform (d.f.t.) is extended considerably. This is accomplished by performing the cyclic convolution, required by Winograd's method, by a fast transform over certain complex integer fields developed previously by the authors. This new algorithm requires fewer multiplications than either the standard fast Fourier transform (f.f.t.) or Winograd's more conventional algorithm.

14. I.S. Reed, and T.K. Truong, "Addendum to Fast Algorithm for Computing Complex Number-Theoretic Transforms," Electronic Letters, Vol. 14, No. 7, 30th March 1978, pp. 231-232.

Abstract - Proof is given of a result previously stated without proof in [4].

15. I.S. Reed, and T.K. Truong, "Fast Mersenne-Prime Transforms for Digital Filtering," Proceeding IEE, Vol. 125, No. 5, May 1978, pp. 433-440.

Abstract - It is shown that Winograd's algorithm can be used to compute an integer transform over GF(q), where q is a Mersenne prime. This new algorithm requires fewer multiplications than the conventional fast Fourier transform (f.f.t). The transform over GF(q) can be implemented readily on a digital computer. This fact makes it possible to more easily encode b.c.h. and r.s. codes.

16. I.S. Reed, T.K. Truong, C.M. Chang and Y.S. Kwoh, "3-D Reconstruction for Diverging X-Ray Beams," IEEE Trans. on Nuclear Science, Vol. NS-25, No. 3, June 1978, pp. 1006-1011.

Abstract - It is shown here that the fast digital convolution technique used for parallel x-ray beams can be used also to reconstruct a density function for diverging x-ray beams. This techqniue when combined with what was called previously a generalized $|\omega|$-filter yields good accuracy, a flexibility to cope with noise and a substantial reduction in the x-ray dosage. Finite field transforms and zero-order interpolation can be used also to improve the speed of the x-ray reconstruction process. Tests based on these methods are performed on an ideal phantom. A detailed comparison is made between a system using diverging beams, and a system using parallel beams with simulated data.

17. I.S. Reed, T.K. Truong and R.L. Miller, "Correction to Fast Algorithm for Computing Complex-Theoretic Transform," Electronic Letters, Vol. 14, No. 13, June 1978, p. 411.

Abstract - This letter corrects an incorrect statement in a previously published letter [4].

18. I.S. Reed, T.K. Truong and R.L. Miller, "A Fast Algorithm for Computing a Primitive 2^{p+1} p-th Root of Unity in GF($(2^p-1)^2$)," Electronic Letters, Vol. 14, No. 15, 20th July, 1978, pp. 493-494.

Abstract - A quick method is developed to find an element or order $2^{p+1}p$ in the finite field GF(q^2), where $q = 2^p-1$ is a Mersenne prime. Such an element is needed to implement complex integer transforms of length $2^k p$ over GF(q^2) where $3 \leq k \leq p+1$.

19. B. Benjauthrit, and I.S. Reed, "On the Fundamental Structure of Galois Switching Functions," IEEE Trans. on Computers, Vol. C-27, No. 8, August 1978, pp. 757-762.

Abstract - It is shown in this paper that the fundamental structure of Galois switching functions follows naturally from that of Boolean switching functions. An expanded formula for deriving multinomial Galois switching functions is provided with illustrations of its application.

20. I.S. Reed, T.K. Truong and R.L. Miller, "A Simple Method for Computing Elements of order $2^k \cdot n$, where $n | 2^{p-1}-1$ and $2 \leq k \leq p+1$ in $GF((2p-1)^2)$," Electronic Letters, Vol. 14, No. 21, Oct. 12th, 1978, pp. 697-698.

Abstract - A simple method is developed for computing elements of order $2^k n$, where n $2^{p-1}-1$ and $2 \leq k \leq p+1$, in the Galois field $GF(q^2)$, and $q = 2^p-1$ is a Mersenne prime. Such primitive elements are needed to implement complex number-theoretic transforms.

21. I.S. Reed and T.K. Truong, "A Fast Computation of Complex Convolution Using a Hybrid Transform," IEEE Trans. Acoustics, Speech, and Signal Processing, Vol. ASSP-26, No. 6, December 1978, pp. 566-570.

Abstract - In this paper it is shown that the cyclic convolution of complex values can be performed by a hybrid transform. This transform is a combination of a Winograd algorithm and a fast complex integer transform developed previously by the authors. This new hybrid algorithm requires fewer multiplications than any previously known algorithm.

22. I.S. Reed and T.K. Truong, "A Simple Proof of the Continued Fraction Algorithm for Decoding Reed-Solomon Codes," Proceedings IEE, Vol. 125, No. 12, December 1978, pp. 1318-1320.

Abstract - It was shown recently that BCH and RS codes can be implemented by Berlekamp's algorithm using continued fraction approximations. A simple transparent proof of Berlekamp's algorithm that uses such a development is given in this paper.

23. I.S. Reed, T.K. Truong, and B. Benjauthrit, "On Decoding of Reed-Solomon Codes Over GF(32) and GF(64) Using the Transform Techniques of Winograd," National Telecommunications Conference, Birmingham, Alabama, December 1978, pp. 20.4.1-20.4.7.

Abstract - The Winograd algorithm over the complex number field is modified to compute a Fourier-like transform over Galois field GF(2^n), where n = 5,6, such a transform can be used to encode and decode Reed-Solomon (RS) codes of length 2^n-1.

24. I.S. Reed, W.V. Glenn, G.M. Chang, T.K. Truong and C.M. Chang, "Wiener Filtering of Successive Overlapping Sections of an X-Ray Reconstruction," IEEE Trans. on Biomedical Engineering, Vol. BME-27, No. 2, February 1979, pp. 101-107.

Abstract - In this paper, a technique is developed to improve the image quality of an object in three-dimensional reconstruction by a weighted average of successive overlapping two-dimensional sections of the object. It is demonstrated that the signal-to-noise ratio of a two-dimensional picture can be improved by roughly a factor of 2 for typical x-ray beam shapes.

25. I.S. Reed, T.K. Truong and R.L. Miller, "Correction to Fast Mersenne Prime Transforms for Digital Filters," Proceedings IEE, Vol. 126, No. 2, February 1979, p. 203.

Abstract - Some of the results in Appendix 8.3 of Reference 15 are incorrect. In this letter, we give the correct results.

26. I.S. Reed, W.V. Glenn, C.M. Chang, T.K. Truong and Y.S. Kwoh, "Dose Reduction in X-Ray Computed Tomography Using a Generalized Filter," IEEE Trans. on Nuclear Science, Vol. NS-26, No. 2, April 1979, pp.2904-2909.

Abstract - Previously with the use of computerized phantoms and simulation, it was conjectured that the x-ray dosage could be reduced by using the appropriate generalized $|\omega|$-filter for x-ray reconstruction. In this paper, this conjecture has been confirmed by experiments that use data from an EMI 5005 CT-scanner. Explicitly it is shown that the x-ray dosage can be lowered to 1/11 of the standard dosage while still maintaining a reconstruction accuracy which is acceptable for some applications.

27. I.S. Reed and T.K. Truong, "A New Hybrid Algorithm for Computing a Fast Discrete Fourier Transform," IEEE Trans. on Computers, Vol. C-28, No. 7, July 1979, pp. 487-492.

Abstract - In this paper for certain long transform lengths, Winograd's algorithm for computing the discrete Fourier transform (DFT) is extended considerably. This is accomplished by performing the cyclic convolution, required by Winograd's method, with the Mersenne prime number-theoretic transform developed originally by Rader. This new algorithm requires fewer multiplications than either the standard fast Fourier transform (FFT) or Winograd's more conventional algorithm. However, more additions are required.

28. I.S. Reed, T.K. Truong and R.L. Miller, "Decoding of B.C.H. and R.S. Codes with Errors and Erasures Using Continued Fractions," Electronic Letters, 16th August 1979, Vol. 15, No. 17, pp. 542-544.

Abstract - Using continued fractions, a simplified algorithm for decoding B.C.H. and R.S. codes is developed that corrects both erasures and errors on a finite field $GF(q^m)$. The decoding method is a modification of the Forney-Berlekamp technique. It is believed that the present scheme is both simpler to understand and to implement than more conventional algorithms.

29. R.L. Miller, I.S. Reed and T.K. Truong, "Simplified Algorithm for Correcting Both Errors and Erasures of Reed-Solomon Codes," Proc. IEE, Vol. 126, No. 10, October 1979, pp. 961-963.

Abstract - Using a finite-field transform, a simplified algorithm for decoding Reed-Solomon codes is developed to correct erasures as well as errors over the finite-field $GF(q^m)$, where q is a prime and m is an integer. If the finite-field transform is a fast transform, this decoder can be faster and simpler than a decoder that uses more conventional methods.

30. I.S. Reed, T.K. Truong and R.L. Miller, "A New Algorithm for Computing Primitive Elements in the Field of Gaussian Complex Integers Modulo a Mersenne Prime," IEEE Trans. on Acoustics, Speech and Signal Processing, Vol. ASSP-27, No. 5, Oct. 1979, pp. 561-563.

Abstract - A new method is developed to find primitive elements in the Galois field of q^2 elements $GF(q^2)$, where q is a Mersenne prime. Such primitive elements are needed to implement transforms over $GF(q^2)$.

31. R.L. Miller, T.K. Truong and I.S. Reed, "Fast Algorithm for Encoding the (255,223) Reed-Solomon Code over GF(2^8)," Electronics Letters, 13th March, 1980, Vol. 16, No. 6, pp. 222-223.

Abstract - A new scheme for reducing the numerical complexity of the standard Reed-Solomon (RS) encoding algorithm is developed. As an example, the encoding of a (255,223) R.S. code (NASA standard for concatenation with convolutional codes) is shown to require 75% fewer multiplications and 61% fewer additions than the conventional method of computation.

32. I.S. Reed, W.V. Glenn, Y.S. Kwoh, T.K. Truong and C.M. Chang, "X-Ray Reconstruction of the Spinal Cord Using Bone Suppression," IEEE Trans. on Biomedical Engineering, Vol. BME-27, No. 6, June 1980, pp. 293-298.

Abstract - In this paper, a new method is developed for obtaining an x-ray reconstruction of the soft tissue detail of the spinal canal. By removing the dominant effects of the bony vertebral body within the projection actual clinical data, higher quality images of the residual soft tissues components can be reconstructed. The intent is a direct visualization of the spinal cord without the need for water-soluble contrast (e.g., Metrizamide) to be installed through a lumbar or cervical puncture. This technique for bone suppresssion also has potential for improving visualization of the interior of the mastoid cavities in the head.

33. I.S. Reed, R.L. Miller and T.K. Truong, "Efficient Program for Decoding the (255,233) Reed-Solomon Code over GF(2^8) with both Errors and Erasures Using Transform Decoding," Proc. IEE, Vol. 127, Pt. E, No. 4, July 1980, pp. 136-142.

Abstract - To decode a (255,223) Reed-Solomon code over GF(2^8), a fast Fourier-like transform over GF(2^8) has been developed to compute the syndromes and the error-erasure vectors of the transmitted code words. This new simplified transform decoder is implemented in a program on a digital computer. The (255,223) Reed-Solomon code over GF(2^8) is being proposed as a NASA standard for concatenation with a (7, ½) conventional code. In a simulation, random code words were corrupted by random error and erasure patterns, and decoded whenever theoretically possible. A matrix of execution times for this new transform decoder under varying sets of errors and erasure patterns is included in the paper. This matrix demonstrates that the speed of the new decoder is between three and seven times faster than the software R-S decoder developed previously by NASA.

34. I.S. Reed, W.V. Glenn, Y.S.Kwoh and T.K. Truong, "A Bandpass Filter for the Enhancement of an X-Ray Reconstruction of the Tissue in the Spinal Canal," IEEE Trans. on Biomedical Engineering, Vol. BME-27, No. 12, December 1980, pp. 736-738.

Abstract - In this communication, a new bandpass reconstruction filter is developed to partially remove the low spatial frequencies of the bone and the soft tissue in an X-ray reconstruction of a lumbar spine. This partial removal of the low frequencies suppresses the bony vertebral body and the soft tissue components within the projections of actual clinical data. It also has the effect of enhancing the sharp edges of the fatty tissue surrounding the spinal cord region. The intent of this effort is to directly visualize the spinal cord without the need for water-soluble contrast (e.g., metrizamide) to be installed through lumbar punctures.

35. T.K. Truong, I.S. Reed, R. Lipes and C. Wu," On the Application of a Fast Polynomial Transform and the Chinese Remainder Theorem to Compute a Two-Dimensional Convolution," IEEE Trans. on Acoustics, Speech and Signal Processing, Vol. ASSP-29, No. 1, Feb. 1981, pp. 91-97.

Abstract - In this paper, a fast algorithm is developed to compute two-dimensional convolutions of an array of $d_1 \times d_2$ complex number points where $d_2 = 2^m$ and $d_1 = 2^{m-r+1}$ for some $1 < r < m$. This new algorithm requires fewer multiplications and about the same number of additions as the conventional FFT method for computing the two-dimensional convolution. It also has the advantage that the operation of transposing the matrix of data can be avoided.

36. R.L. Miller, I.S. Reed and T.K. Truong, "A Theorem for Computing Primitive Elements in the Field of Complex Integers of a Characteristic Mersenne Prime," IEEE Trans. on Acoustics, Speech, and Signal Processing, Vol. ASSP-29, No. 1, February 1981, pp. 119-120.

Abstract - A method developed previously [30] for computing primitive elements in $GF(q^2)$, where q is a Mersenne prime, is shown not to generalize to other Galois fields. The method will be successful in finding primitive elements of $GF(q^n)$ if and only if q is a Mersenne prime and $n = 2$.

37. I.S. Reed, T.K. Truong, B. Benjauthrit, and C. Wu, "A Fast Algorithm for Computing a Complex-Number Theoretic Transform for Long Sequences," IEEE Trans. on Acoustics, Speech, and Signal Processing, Vol. ASSP-29, No. 1, February 1981, pp. 122-124.

Abstract - This correspondence describes an algorithm for computing a complex-number theoretic transform of long sequences. Such a transform technique can be used to compute the convolution of two sequences of complex numbers. Emphasis is given to a transform of length $9 \cdot 8 \cdot 31 = 2232$. Such a transform can be used to perform the matched-filter correlation of raw radar-echo data and the range response function for producing images from synthetic aperture radar (SAR) data.

38. I.S. Reed, T.K. Truong, R.L. Miller and J. P. Huang, "Fast Transforms for Decoding Reed-Solomon Codes," IEE Proc., Vol. 128, Pt. F, No. 1, February 1981, pp. 9-14.

Abstract - In the paper it is shown that the Chinese remainder theorem when coupled with a modification of Winograd's method can be used to compute Fourier-like transforms over $GF(2^m)$, where $m = 2,3,\ldots,8$. These new transform techniques are to decode Reed-Solomon codes of block length 2^m-1. The results are shown to be more efficient than the more conventional method.

39. I.S. Reed, H.M. Shao, and T.K. Truong, "Fast Polynomial Transform and its Implementation by Computer," IEE Proc., Vol. 128, Pt. E, No. 1, March 1981, pp. 50-60.

Abstract - Recently a new algorithm was developed to compute two-dimensional cyclic convolution by what is called the FPT (fast polynomial transform) algorithm. In this paper this new algorithm is further studied and implemented on a general purpose computer. Methods to cope with finite core memory limitations are presented and actual computational speed performances are listed.

40. I.S. Reed, T.K.Truong, and B. Benjauthrit, "Addendum to a New Hybrid Algorithm for Computing a Fast Discrete Fourier Transform," IEEE Trans. on Computers, Vol. C-30, No. 6, June 1981, pp. 453-454.

Abstract - Recently, the authors [27] proposed a hybrid algorithm for computing the discrete Fourier transform (DFT) of certain long transform lengths. In that technique, a Winograd-type algorithm was used in conjunction with the Mersenne prime-number theoretic transform to perform a DFT. Even though this technique requires fewer multiplications than either the standard fast Fourier transform (FFT)

or Winograd's more conventional algorithm, it increases the number of additions considerably. In this letter it is proposed to use Winograd's algorithm for computing the Mersenne prime-number theoretic transform in the transform portion of the hybrid algorithm. It is shown that this can reduce significantly the number of additions while still maintaining about the same number of multiplications.

41. Y.S. Kwoh, I.S. Reed, T.K. Truong and W.V. Glenn, "A New CT Collimator for Producing Two Simultaneous Overlapping Slices from One Scan," IEEE Trans. on Biomedical Engineering, Vol. BME-28, No. 9, September 1981, pp. 664-667.

Abstract - In this paper, a modification of the EMI CT 5005 collimator is used to simultaneously produce two overlapping two-dimensional sections of the object from one scan. Such a new collimator not only achieves a speed improvement in the generation of successive overlapping sections, but also yields a reduction of the X-ray dosage used by the standard EMI CT 5005 collimator. It is demonstrated that the quality of the images from these two slices almost equals the quality of the images that are produced by the EMI CT 5005 collimator from two separate scans.

42. H.M. Shao, I.S. Reed, T.K. Truong and Y.S. Kwoh, "An Improved CT-Aided Stereotactic Neurosurgery Technique," Proc. of the Fifth Annual Symposium on Computer Applications in Medical Care, November 1981, pp. 591-595.

Abstract - In this paper, computer software is developed for a specially designed head mounted frame that is used in neurosurgery. This system is applied to stereotactic surgery. It is shown to provide a simple, fast and accurate tool for brain neurosurgery.

43. D.K. Kravitz and I.S. Reed, "Extension of RSA Crypto-Structure: A Galois Approach," Electronics Letters, 18th March 1983, Vol. 18, No. 6, pp. 255-256.

Abstract - The Euler totient function and Euler-Fermat theorem utilized in the RSA scheme are extended from the integers to polynomials over finite fields. The new scheme is suited for both privacy and authentication implementations, as is its predecessor. The security of the system rests in part on the difficulty of determining the degrees of the irreducible factors of a high-degree polynomial.

44. T.K. Truong, I.S. Reed, C.-S. Yeh and H.M. Shao, "A Parallel VLSI Architecture for A Digital Filter of Arbitrary Length Using Fermat Number Transforms," Proceedings of 1982 IEEE International Conference on Circuits and Computers, Sept. 28 - Oct. 1, 1982, New York, pp. 574-578.

Abstract - In this paper a parallel and pipeline architecture is developed to compute the linear convolution of two sequences of arbitrary lengths using the Fermat number transform (FNT). Such a new architecture is developed to realize the overlap-save method using one FNT and several reverse FNT's of 128 points. The generalized overlap-save method alleviates the usual dynamic range limitation in FNT's of long transform lengths. Its architecture is regular, simple, expandable, and naturally suitable for VLSI implementation.

45. T.K. Truong, I.S. Reed, and C.-S. Yeh, "A Parallel Architecture for Computing Cyclic Convolutions," Proceedings of the Trends in Electronics Conference, Dec. 6-8, 1982, Hong Kong, pp. 1-6.

Abstract - In this paper, a parallel architectural structure is developed to compute one-dimensional cyclic convolutions. This structure is based on the Chinese remainder theorem and Kung's systolic array. To compute a d-point cyclic convolution the structure needs d/2 inner product cells. The utilization of this structure is high. Also it is simple and regular, and therefore suitable for VLSI implementation.

46. T.K. Truong, L.J. Deutsch, I.S. Reed, I.S. Hsu, K. Wang, and C.-S. Yeh, "The VLSI Design of a Reed-Solomon Encoder Using Berlekamp's Bit-Serial Multiplier Algorithm," Proceedings of the Third Caltech Conference on Very Large Scale Integration, Calif. Institute of Technolcgy, Pasadena, Calif., 1983, pp. 303-329.

Abstract - E.R. Berlekamp has developed for the Jet Propulsion Laboratory a bit-serial multiplication algorithm for the encoding of Reed-Solomon (RS) codes, using a dual basis over a Galois field. The conventional RS-encoder for long codes often requires look-up tables to perform the multiplication of two field elements. Berlekamp's algorithm requires only shifting and exclusive-OR operations. It is shown in this paper that the new dual-basis (255, 223) RS-encoder can be realized readily on a single VLSI chip with NMOS technology.

47. I.S. Reed, C.-S. Yeh, and T.K. Truong, "A VLSI Architecture for Digital Filters Using Complex Number-Theoretic Transforms," Proceedings 1983 International Conference on Acoustics, Speech, and Signal Processing, April 14-16, 1983, Boston, Mass., pp. 923-926.

Abstract - In this paper a parallel architecture is developed to realize a digital filter. First a systolic array is used to compute a 248-point complex number-theoretic transform (CNT). Next an algorithm is developed to realize a digital filter that uses 248-point CNT's and a generalization of the overlap-save method.

This algorithm solves the conflict between long transform lengths and a wide dynamic range associated with the number-theoretic transform. Finally this algorithm is mapped to a parallel architecture. This architecture is simple, regular and expandable, and, hence, is suitable for VLSI implementation.

48. I.S. Reed, and T.K. Truong, "New Syndrome Decoder for (n,1) Convolutional Codes," Electronics Letters, Vol. 19, No. 9, 25th April, 1983, pp. 344-346.

Abstract - This letter presents a new syndrome decoding algorithm for the (n,1) convolutional codes (CC) that is different and simpler than the previous syndrome decoding algorithm of Schalkwijk and Vinck. The new technique uses the general solution of the polynomial linear Diophantine equation for the error polynomial vector E(D). A recursive, Viterbi-like, algorithm is developed to find the minimum weight error vector $\hat{E}(D)$. An example is given for the binary non-systematic (2,1) CC.

B. Dissertations and Abstracts

49. Y.S. Kwoh, Application of Finite Field Transforms to Image Processing and X-Ray Reconstruction, Ph.D. Dissertation, University of Southern California, January 1977.

Abstract

This dissertation develops and utilizes an important class of finite field transforms which are similar to the discrete Fourier transform. Specifically a transform is defined here over GF(p), where p is a prime of the form $k \cdot 2^n+1$, where k and n are integers.

In this thesis the above transform is used first to filter a two-dimensiona picture. Then the results are compared with the standard FFT.

Another area of image processing involves the reconstruction of an x-ray image from one-dimensional projection data. It is also applied to 3-D reconstruction with a consequent speed and accuracy advantage over the conventional method.

Important problem of 3-D reconstruction which arose in the above are also studied in detail. These include a development of a new generalized $|\omega|$-filter. The parameters of the generalized $|\omega|$-filter presented here have good reconstruction accuracy as well as flexibility.

Also, it turns out that the development of the generalized $|\omega|$-filter leads to a very impressive result, namely, a substantial reduction of x-ray dosage. Hence the combination of the finite field transform and the generalized $|\omega|$-filter promise to yield significant improvements over existing systems.

50. K.Y. Liu, Efficient Digital Transform Algorithms and Architectures for Signal Processing and Error Correcting Codes, Ph.D. Dissertation, University of Southern California, June 1977.

Abstract

Several classes of efficient digital transform algorithms and architectures that have application to dqgital signal processing and error-correcting codes are presented in this dissertation.

It is shown that both high radix and real-valued-input, fast-Fourier-transform (FFT) algorithms can be used with number-theoretic transforms on the finite field $GF(q^2)$, where $q = 2^p-1$ is a Mersenne prime, when the transform length d divides 2^{p+1}. Also shown is a highly efficient mixed-radix FFT over $GF(q^2)$ for $d = 2^k p$ with $0 \leq k \leq p+1$. This new FFT algorithm requires substantially fewer multiplications than the conventional FFT and the Winograd FFT algorithm over the complex numbers.

A special number-theoretic transform that can be computed, using a high-radix FFT, is defined on primes of the form $(2^n-1)2^n+1$. Also included are methods for finding these primes and the primitive d^{th} roots of unity in the finite field of integers modulo such primes.

A high-radix FFT with generator $\gamma = 3$ over $GF(F_n)$ where $F_n = 2^{2^n}+1$ is a Fermat prime is found to be useful for the fast encoding and decoding of Reed-Solomon (RS) codes. A new class of highly efficient LSI logic structures, called assembly-line structures, are studied. Real-time digital signal processors can be constructed by combining specialized LSI chips, utilizing such logic structures.

51. C.M. Chang. 3-D Reconstruction and the Technique of X-Ray Computerized Tomography, Ph.D. dissertation, University of Southern California, July 1979.

Abstract

In this dissertation it is shown that the fast digital convolution technique used for parallel x-ray beams can be used also to reconstruct a density function for diverging x-ray beams. The convolution method when used with a generalized $|\omega|$-filter yields good accuracy and a flexibility to filter unwanted noise. It is shown that the x-ray dosage can be lowered to 1/11 of the standard dosage while still maintaining a reconstruction accuracy that is acceptable for many applications.

An important problem of x-ray computed tomography is to improve the image quality so that the x-ray image can be diagnosed accurately. This problem is studied here in some detail. A technique is developed to improve the CT image quality of an object in 3-D reconstruction by a weighted average of successive overlapping 2-D sections of the object.

Finally, a new method is developed to reconstruct the soft tissue detail of the spinal canal. By removing the dominant effects of the bony vertebral body within the projection data, it is demonstrated that higher quality images of the residual soft tissue components can be reconstructed.

52. David William Kravitz, The Application of Finite Polynomial Rings to Number Theoretic Crypto-Systems, Ph.D. Dissertation, University of Southern California, May 1982.

Abstract

A cryptographic construct is proposed based on traditional information-theoretic and modern computational complexity-theoretic principles. The methodology developed is suitable for the implementation of both conventional symmetric key ciphers, and the recently introduced public-key cryptomechanism characterized by the ability to divulge one of the keys in the matched (encryption, decryption) pair without leading to compromise of the remaining key.

The development hinges on two mathematical means of generalization, namely (a) the transformation of the message space from Z_p to $Z_p[x]/(g(x))$ where $g(x)$ is any irreducible polynomial over Z_p, the finite field of integers modulo a prime number p, to $Z_p[x]/(f(x))$ where $f(x) = \prod_j g_j(x)$, the product of distinct irreducible polynomials over Z_p; and (b) the direct summation of such quotient ring terms, isomorphically realized by invoking the Chinese remainder theorem for integers.

The newly endowed polynomial structure is then exploited by concatenating these ciphers with a data scrambling technique.

Incorporation of the resulting cryptostructures into the demanding environment of modern multi-user secure communications networks is discussed and analyzed.

53. Howard M. Shao, Techniques for Signal Processing of Image Data, Ph.D. Dissertation, University of Southern California, May 1983.

Abstract

Techniques for processing images have become of increasing interest in recent years. Among them, very often, a two-dimensional filtering operation has been required.

The commonly used FFT method to compute a 2-D convolution is considered to involve too many complex multiplications as well as an undesired matrix transpose operation. New algorithms are being developed to cope with such problems.

It was first shown in the work of Nussbaumer and Quandalle [1-3] that a certain type of polynomial transform could be used to compute two-dimensional convolutions. Truong and Reed [4] modified the polynomial transform with the Chinese remainder theorem to obtain a more efficient algorithm. By using a new factorization of the modulus, a new algorithm, called the Fast Polynomial Transform (FPT) was developed. This technique takes advantage of an FFT-type architectural structure to compute the 2-D convolution more rapidly than can be accomplished with the standard 2-D FFT structure.

In this dissertation, the fast polynomial transform is further elaborated and implemented on a general purpose computer. It is shown also how to realize a high speed array processor. Methods to cope with finite core memory limitations are prevented and actual speed performances are obtained. Since 50% of the complex multiplications in a standard 2-D FFT are replaced by word shifts in the FPT, experiments show that the FPT has a 20% speed improvement over the ordinary 2-D FFT for computing 2-D Convolutions.

The FPT algorithm developed in this thesis has been successfully applied to the synthetic aperture radar (SAR) imaging problem [5]. This involves the computation of two-dimensional cross correlation of radar echo data with the response or point spread function of a point target.

Another potentially important application is the detection of a moving target in optical image data by a three-dimensional space-time filter bank. Herein an optimal 3-D filter is developed for detecting optical paths. Performances is computed on the assumption of a Markov clutter model. The new algorithm shows a dramatic increase in detectability as a function of target velocity. A three-dimensional FPT algorithm is also developed to perform the 3-D space-time filtering. This method improves the computation speed of 3-D digital filtering significantly.

Another often more difficult task than the above is the detection of weak stationary targets in optical image data. The method of standard detection is often unsatisfactory. Thus in this thesis an optimum adaptive algorithm is developed for the detection of a signal image in a scene with a correlated reference scene without signal. The algorithm is implemented with a computer program utilizing actual image data. Experiments show that better than an average 6 dB improvment can be achieved over the method of direct correlation.

For real world applications both the 3-D space-time filtering and the optimum adaptive filtering require an excessive amount of computation. The fast polynomial transform and other similar techniques are efficient computing algorithms for improving digital signal processing. It is expected that the results of this thesis will lead to the development of more practical and useful techniques for image and data processing problems.

54. Chiunn-Shyong Yeh, Parallel VLSI Architectures of Signal and Communication Processors, Ph.D. Dissertation, University of Southern California, June 1983.

Abstract

In this dissertation VLSI architectures of signal and communication processors are developed. The increasing complexity of VLSI devices is a challenge to both architecture and circuit designers. The development costs and turnaround time are extremely important for designing custom VLSI devices. Herein approaches and the difficulties associated with the design of the VLSI device are investigated. The properties that a VLSI architecture should possess in order to minimize the design costs are discussed. The important properties of VLSI architectures that need to be addressed are interconnects, regularity, control, modularity and concurrency.

In this dissertation, the VLSI architectures of three signal processors are developed. The first design is a VLSI architecture for the arithmetic of the finite field $GF(2^m)$ of 2^m elements. Algorithms are derived to perform the multiplication and inverse in the finite field $GF(2^m)$. Then two architectures are designed to realize the multiplication algorithm. These multipliers then are used to design an inversion circuit for the finite field $GF(2^m)$.

The second system is a VLSI architecture for digital filters which uses the Fermat number transform (FNT). A pipeline structure is designed to compute a 128-point FNT. A major drawback of the FNT is the conflict between long transform lengths and a large dynamic range. A generalized overlap-save algorithm is developed to solve the conflict of the FNT. Then a VLSI architecture is designed to realize the generalized overlap-save algorithm for a digital filter using the FNT.

The third design is a VLSI architecture for digital filtering which uses a complex number-theoretic transform (CNT). A one-dimensional array is designed to compute a 248-point CNT. Then a parallel VLSI architecture is designed to realize a digital filter by this CNT and the generalized overlap-save algorithm.

The architectures of these signal and communication processors are simple and modular, and possess the properties of regularity and concurrency. Therefore they are well-suited for implementation in VLSI devices.

element is needed to implement complex integer ...
$2^k p$ over $GF(q^2)$ where $3 \leq k \leq p+1$.

END

FILMED

11-83

DTIC